DDP: A TOOL FOR FAILURE MODE RISK MANAGEMENT

Thomas Gindorf and Steve Cornford
Jet Propulsion Laboratory, California Institute of Technology
Pasadena, CA USA

Abstract

A principal tool under development as part of the NASA Failure Detection and Prevention Program is the Defect Detection and Prevention (DDP) tool. Early application of the DDP tool has shown great promise in providing project decision makers with the basic information and the methodology required to trade off risk with other resources (e.g., cost, schedule). The optimum combination of Preventative measures, Analyses, process Controls, and Tests (PACTs) can be iteratively determined within various resource constraints, and evolves with the project design process. By examination of the residual risk associated with the combinations of PACTs, a balanced approach can be developed for addressing the active failure modes in the hardware under consideration. The DDP process provides a means to perform ongoing technical and programmatic risk management. The overall DDP concept has previously been described in the open literature. This paper addresses the implementation process, the latest tool developments, and provides some generalized numerical examples intended to foster a deeper understanding of the DDP process and NASA's Risk Balancing Profiles, as well as the utility of the DDP tool for NASA's Integrated Synthesis Environment and the Collaborative Engineering Environment.

Introduction

Failure modes can be activated on spacecraft hardware as a result of specific combinations of the technology selected, its application, and its exposure during the application. The consequences of these active failure modes (FMs) pose risk to proper operations of the hardware which projects must carefully manage to ensure mission success. Before the hardware and the technology have been defined, active failure modes cannot be confidently identified. Risk Balancing Profiles[1], can be used early in the program life cycle before designs have been fully developed to define assurance activities considered appropriate for generic risk control (Figure 1). As the hardware design evolves, details about the planned implementation emerge allowing active failure modes to be more confidently identified and more specific risk controls can be implemented.

The Defect Detection and Prevention (DDP) tool is being developed to assist in managing risk at the active failure mode level. The DDP tool is a model driven computer based tool, which provides a basis for interaction in the Intelligent Synthesis Environment (ISE) and the Collaborative Engineering Environment (CEE) being deployed for NASA Spacecraft development.[2]

The DDP tool is used to refine the decisions and assumptions made in earlier formulations of Risk Management and Mission Assurance planning. The DDP tool is ideally utilized before manufacturing, integration, and testing has actually begun to balance the risk, optimize efficiency, and validate previous planning. Equally important, the DDP tool provides a method to continually iterate designs and their associated resources on the basis of risk management of active failure modes. The DDP tool development is part of an overall Failure Detection and Prevention Program sponsored by NASA's Office of Safety and Mission Assurance.

DDP - What Is It?

Simply stated, DDP is an interactive tool that establishes the relative significance of

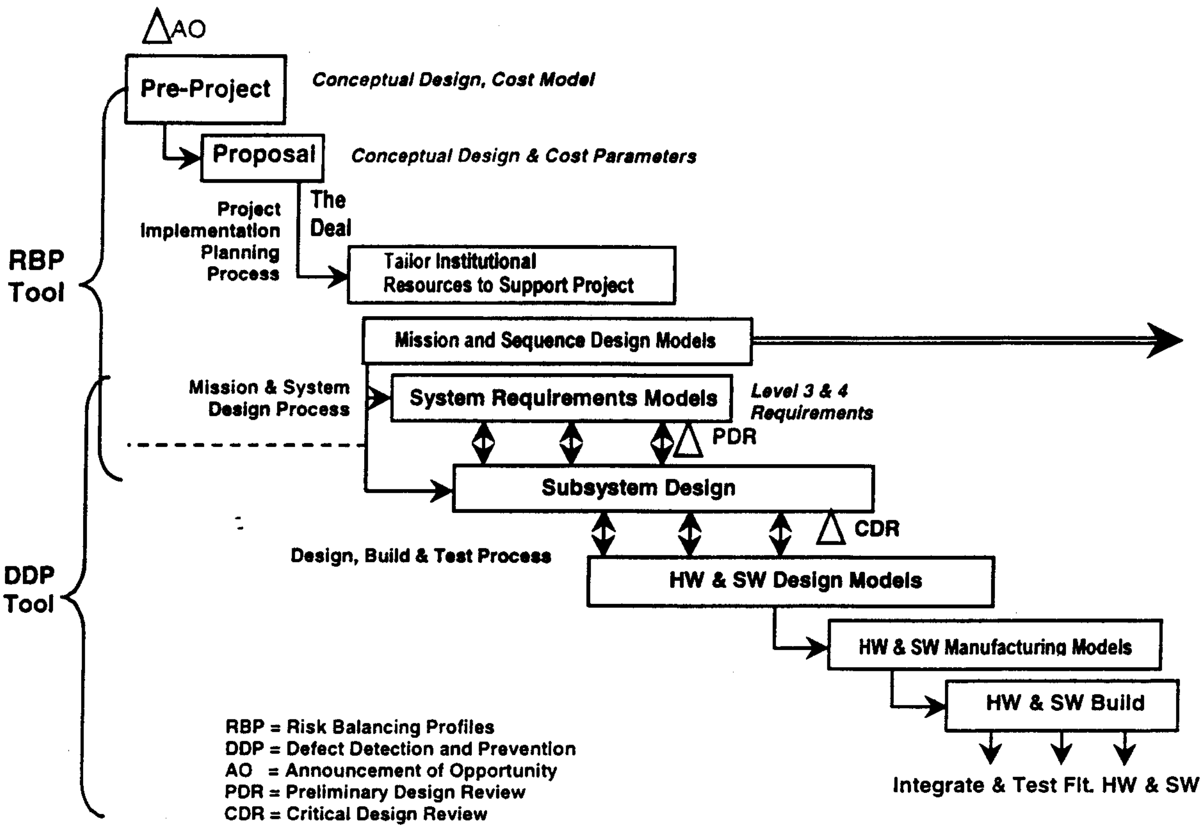
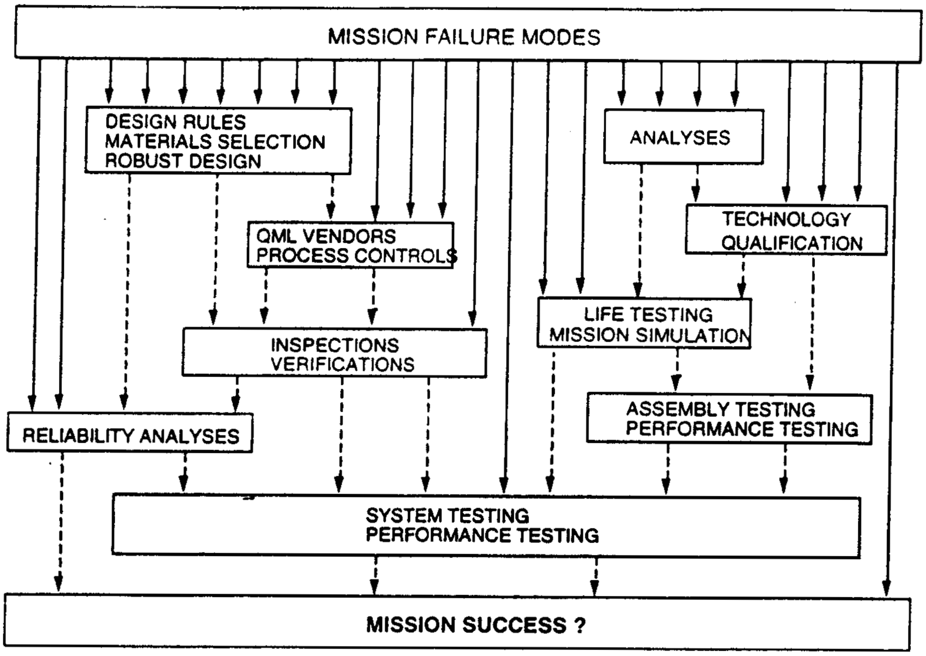

AO
Pre-Project
Conceptual Design, Cost Model
Proposal
Conceptual Design & Cost Parameters
Project Implementation Planning Process
The Deal
Tailor Institutional Resources to Support Project
RBP Tool
Mission and Sequence Design Models
Mission & System Design Process
System Requirements Models
Level 3 & 4 Requirements
PDR
Subsystem Design
CDR
Design, Build & Test Process
DDP Tool
HW & SW Design Models
HW & SW Manufacturing Models
HW & SW Build
Integrate & Test Flt. HW & SW
RBP = Risk Balancing Profiles
DDP = Defect Detection and Prevention
AO = Announcement of Opportunity
PDR = Preliminary Design Review
CDR = Critical Design Review

Figure 1. Typical Project Process Flow

specific FMs by evaluating the impact of their occurance on the mission requirements. The tool evaluates the effectiveness of various Preventive Measures, Analyses, Process Controls and Tests (PACTs) options allowing one to determine an optimum set to manage the risk within the resource constraints of the particular project.

Figure 2 depicts a collection of FMs that can either be detected or prevented (or not) by a set of PACTs. The potential presence of these failure modes is illustrated by solid arrows, where the dashed arrows represent "escapes" (undetected or prevented) from a given PACT and the disappearance of an arrow represents the failure mode being either detected or prevented. The PACTs in this example are only generically identified. Two situations that are obvious from Figure 2 are: 1) Some failures escape and aren't detected or prevented at all by the PACTs portrayed (the line on the far right); and(2) Some failures are detected or prevented over and over. Neither of these conditions is desirable. In the first case, the FM will either destroy or diminish mission success. In the second case, schedule and cost inefficiencies usually result. DDP is a tool that facilitates optimization by establishing the appropriate degree of concern about "escapes" in the PACTs defined and determining the optimum set of PACTs for the resources available.

Figure 3 pictorially defines the relationships between failure modes, requirements and PACTs in the DDP process. A Requirements Matrix (R) is used to establish the weighted impact of FMs "active" on the mission requirements. These weighted FMs are then addressed systematically in an Effectiveness Matrix (E) and the effectiveness of the various PACTs to either prevent or detect them is determined. Each of these PACTs has a resource cost associated with it (e.g., radiation shielding costs mostly mass, while radiation testing cost mostly $ and time). This iterative process between R and E can be exercised as needed in real time in a model-based environment, as depicted in Figure 4.

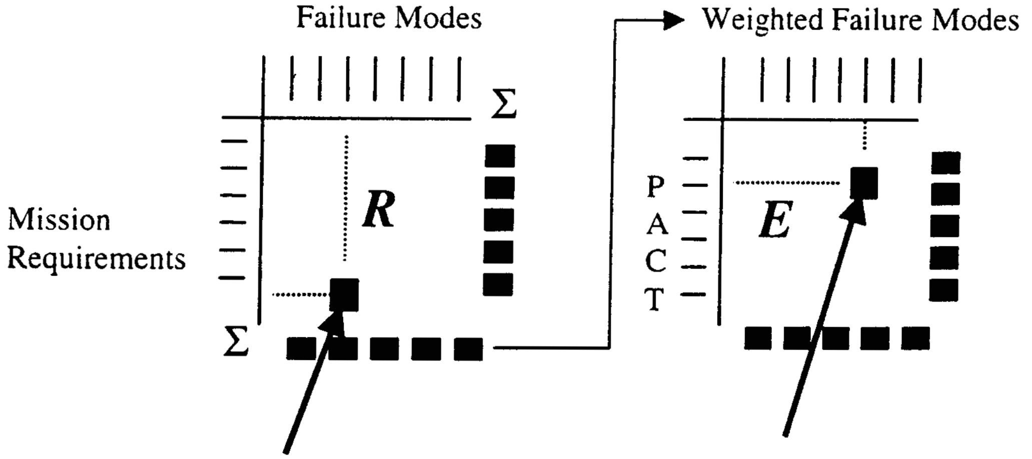


Notes:
1) Each box is a collection of PACTs
2) Dotted lines represent "escapes" - Undetected or un-prevented failure modes
3) Illustrative diagram only - nothing is "to scale"

***PACT*s** - Are everything that could be done (e.g. "toolbox" of prevention/detection options)
Preventative measures (Redundancy, Design Rules, Materials Selection, Software Architecture, etc.)
Analyses (Reliability (Fault Tree Analyses, Failure Mode and Effects Criticality Analysis (FMECA), Worst Case Analysis), Fatigue, Structural, Performance, Electrical SPICE models, etc.)
process Controls (Inspections, Materials purity, QML vendors, Documentation, etc.)
Tests (Environmental, Life, Simulations, Performance, etc.)

FAILURE MODES(FMs)/DEFECTS
Failure is used in its broadest sense: Failure to meet goals/requirements
"Hard" - Cracks, Explosions, Open Circuits, etc.; "Soft" - Resets, Performance Degradations, etc.

Figure 2. Screening Out the Defects



Impact of a given FM on a particular requirement

Effectiveness of a given PACT to detect or prevent a particular FM

Figure 3. Simplified DDP Summary (**DDP utilizes two matrices: the Requirements matrix (*R*) and the Effectiveness matrix (*E*))**

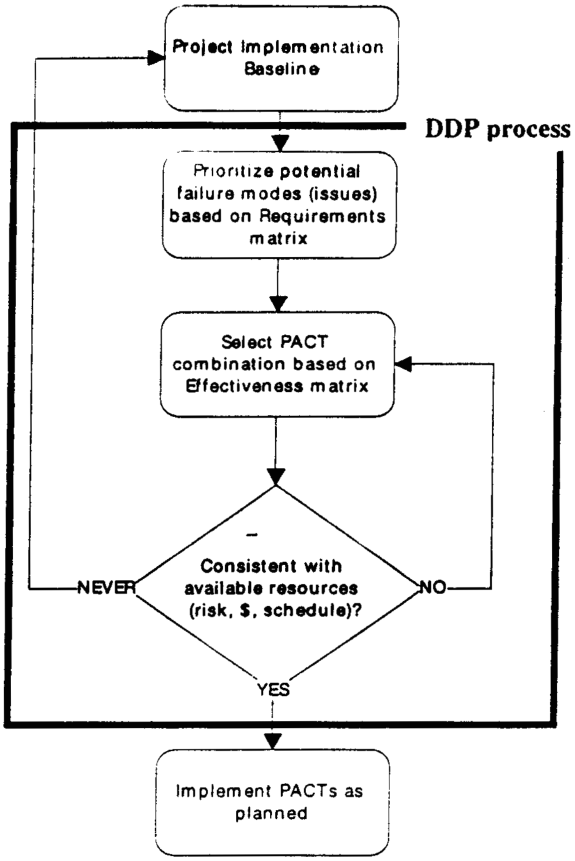

Project Implementation Baseline
DDP process
Prioritize potential failure modes (issues) based on Requirements matrix
Select PACT combination based on Effectiveness matrix
Consistent with available resources (risk, $, schedule)?
NEVER
NO
YES
Implement PACTs as planned

Figure 4. Simplified Summary of the DDP Process

DDP - How Does It Work?

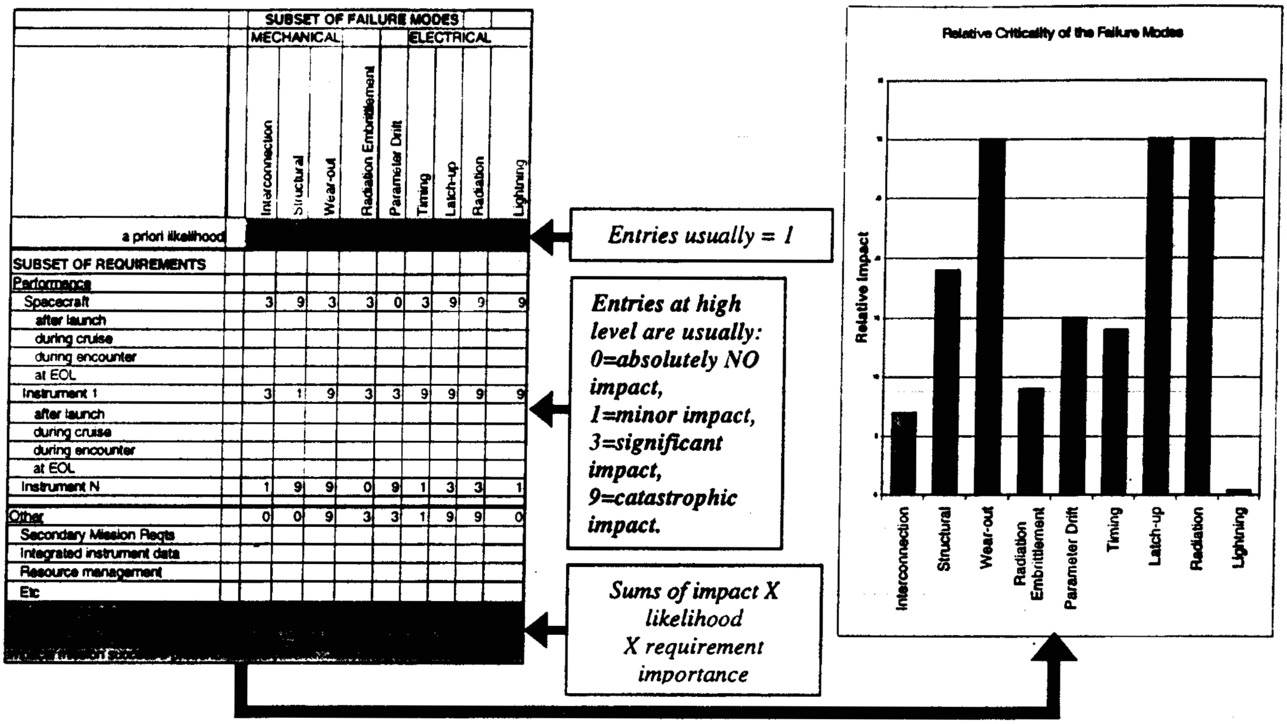
Requirements Matrix:
At the heart of understanding the DDP tool is establishing the impact of the occurrence of each FM to mission success. From a lengthy list of possible FMs, the environment, mission characteristics, and selected hardware technology and architectures are used to screen down to those FM that are"active", or potential, for the mission planned. The potential FMs are then weighted by their likelihood of occurrence if nothing is done about them (usually a certainty!). Their impact on various mission success criteria (or requirements at lower-levels of evaluation) is established using a non-linear scale of significance. In this example the scale can range from 0 for no impact to 9 for catastrophic impact. The product of likelihood of occurrence and impact weights for each FM can then be plotted to determine the relative criticality of the FMs to the success of the mission. This is a relative measure of how much one should "care" about the active FMs (barchart shown in Figure 5).

Effectiveness Matrix:
The weighted FMs are utilized to determine the proper courses of action to manage the risks associated with them. This involves establishing the relative chance that a Failure Mode will go undetected and/or won't be prevented by the various PACTs already planned, or possible. Different PACTs will have different escape probabilities* for different FMs (chance of missing the FM). These escape probabilities are entered into the Effectiveness matrix, which is depicted in Figure 6. By multiplying the escape p~~P~~robabilities from all of the PACTs for each FM, one can obtain the net likelihood of 'escape", or being missed. The resultant risk for an FM is then obtained by taking the product of the impact of the FM on requirements and the ~~its~~ escape probability for each PACT ~~isthe~~ combination considered (column calculations). This process is repeated for each FM. Different combinations of PACTs result in different risk balances, as shown in Figure 7. Note that one can optimize across all PACTs (i.e., start with a 'clean sheet of paper'), or tailor an existing program (i.e., start with one of the combinations in Figure 7 and add/subtract PACTs to reach the desired risk balance).

One can also formulate a figure-of-merit for various PACT combinations based on the extent to which risk is detected/prevented by summing the products of the impact of the FM on requirements and the probability of an individual PACT detecting or preventing the active FMs (1-escape probability). This figure- of-merit can then be used to decide when enough PACTs have been selected or be used to establish a baseline about which one can perform incremental changes (See Figure 6).

*Note: Actual escape probabilities are inserted where they are known (easiest in high volume application). However, generally in ultra low volume applications they are assigned in accord with the legend in Figure 6 by expert opinion (Delphi techniques).

fix font



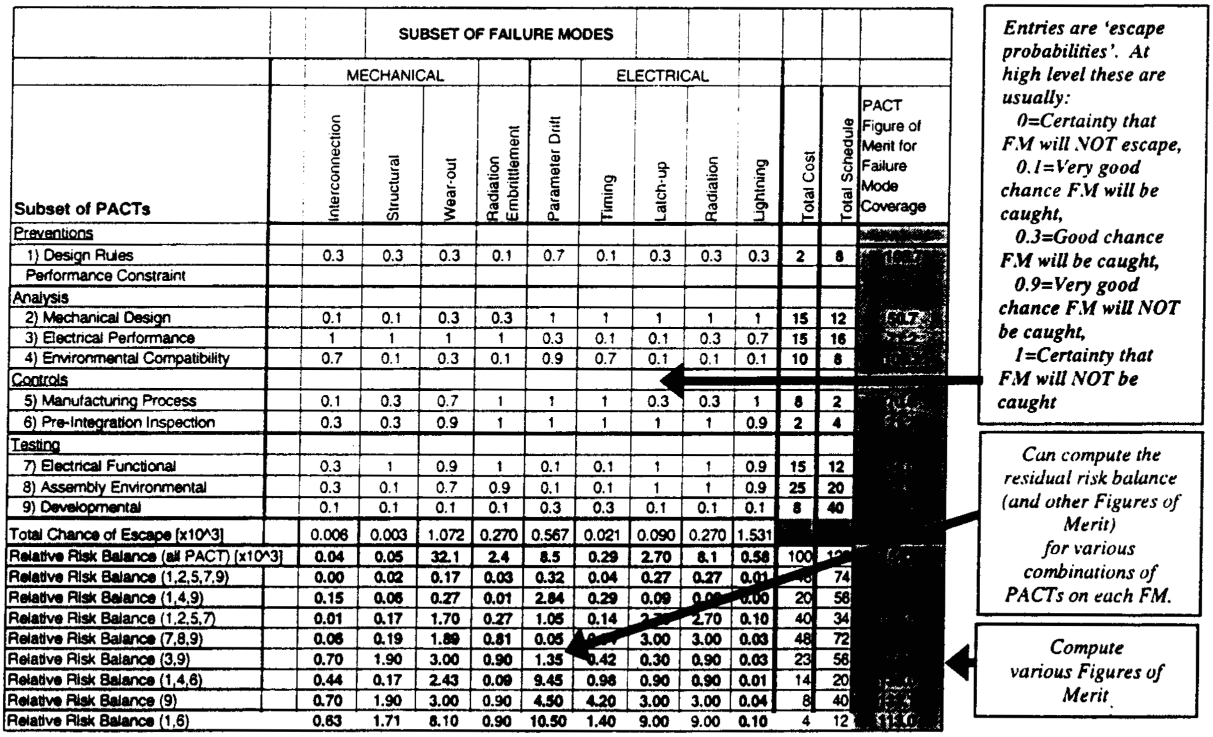
	SUBSET OF FAILURE MODES								
	MECHANICAL				ELECTRICAL				
	Interconnection	Structural	Wear-out	Radiation Embrittlement	Parameter Drift	Timing	Latch-up	Radiation	Lightning
a priori likelihood									
SUBSET OF REQUIREMENTS									
Performance									
Spacecraft	3	9	3	3	0	3	9	9	9
after launch									
during cruise									
during encounter									
at EOL									
Instrument 1	3	1	9	3	3	9	9	9	9
after launch									
during cruise									
during encounter									
at EOL									
Instrument N	1	9	9	0	9	1	3	3	1
Other	0	0	9	3	3	1	9	9	0
Secondary Mission Reqts									
Integrated instrument data									
Resource management									
Etc									

Entries usually = 1

Entries at high level are usually: 0=absolutely NO impact, 1=minor impact, 3=significant impact, 9=catastrophic impact.

Sums of impact X likelihood X requirement importance

Figure 5. DDP Requirements Matrix



	SUBSET OF FAILURE MODES											
	MECHANICAL				ELECTRICAL							
Subset of PACTs	Interconnection	Structural	Wear-out	Radiation Embrittlement	Parameter Drift	Timing	Latch-up	Radiation	Lightning	Total Cost	Total Schedule	PACT Figure of Merit for Failure Mode Coverage
Preventions												
1) Design Rules	0.3	0.3	0.3	0.1	0.7	0.1	0.3	0.3	0.3	2	8	[illegible]
Performance Constraint												
Analysis												
2) Mechanical Design	0.1	0.1	0.3	0.3	1	1	1	1	1	15	12	50.7
3) Electrical Performance	1	1	1	1	0.3	0.1	0.1	0.3	0.7	15	16	[illegible]
4) Environmental Compatibility	0.7	0.1	0.3	0.1	0.9	0.7	0.1	0.1	0.1	10	8	[illegible]
Controls												
5) Manufacturing Process	0.1	0.3	0.7	1	1	1	0.3	0.3	1	8	2	[illegible]
6) Pre-Integration Inspection	0.3	0.3	0.9	1	1	1	1	1	0.9	2	4	
Testing												
7) Electrical Functional	0.3	1	0.9	1	0.1	0.1	1	1	0.9	15	12	
8) Assembly Environmental	0.3	0.1	0.7	0.9	0.1	0.1	1	1	0.9	25	20	
9) Developmental	0.1	0.1	0.1	0.1	0.3	0.3	0.1	0.1	0.1	8	40	
Total Chance of Escape [x10^3]	0.006	0.003	1.072	0.270	0.567	0.021	0.090	0.270	1.531			
Relative Risk Balance (all PACT) [x10^3]	0.04	0.05	32.1	2.4	8.5	0.29	2.70	8.1	0.58	100	[illegible]	
Relative Risk Balance (1,2,5,7,9)	0.00	0.02	0.17	0.03	0.32	0.04	0.27	0.27	0.01	[illegible]	74	
Relative Risk Balance (1,4,9)	0.15	0.06	0.27	0.01	2.84	0.29	0.09	[illegible]	0.00	20	58	
Relative Risk Balance (1,2,5,7)	0.01	0.17	1.70	0.27	1.05	0.14	[illegible]	2.70	0.10	40	34	
Relative Risk Balance (7,8,9)	0.06	0.19	1.89	0.81	0.05	[illegible]	3.00	3.00	0.03	48	72	
Relative Risk Balance (3,9)	0.70	1.90	3.00	0.90	1.35	0.42	0.30	0.90	0.03	23	56	
Relative Risk Balance (1,4,6)	0.44	0.17	2.43	0.09	9.45	0.98	0.90	0.90	0.01	14	20	
Relative Risk Balance (9)	0.70	1.90	3.00	0.90	4.50	4.20	3.00	3.00	0.04	8	40	
Relative Risk Balance (1,6)	0.63	1.71	8.10	0.90	10.50	1.40	9.00	9.00	0.10	4	12	111.0

Entries are 'escape probabilities'. At high level these are usually:
0=Certainty that FM will NOT escape,
0.1=Very good chance FM will be caught,
0.3=Good chance FM will be caught,
0.9=Very good chance FM will NOT be caught,
1=Certainty that FM will NOT be caught

Can compute the residual risk balance (and other Figures of Merit) for various combinations of PACTs on each FM.

Compute various Figures of Merit

Figure 6. DDP Effectiveness Matrix

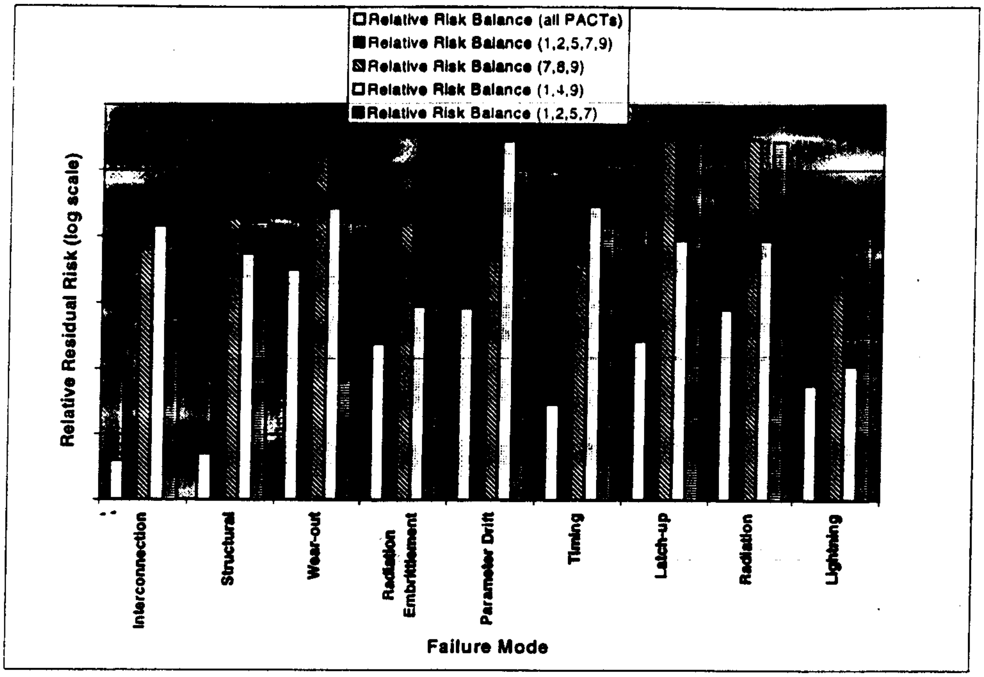


Figure 7. Relative Risk Balance for Selected PACT Combinations

Applying DDP

The DDP process is iterative and begins with high-level requirements, failure modes and PACTs which then are refined and become more specific. For example, in the early stages of a project, the requirements can be rather high-level (e.g., get to Saturn within 5 years), the FMs are also rather high-level (e.g., navigation or propulsion anomalies), and so are the PACTs (e.g., utilize redundancy and a qualification/acceptance program). However, as the design matures, so do the three contributors to the risk balance: requirements, FMs and PACTs. For example, prior to the Preliminary Design Review (PDR) the three contributors have reached lower levels. For example, the requirements look more like 'propulsion system needs to provide xx minutes of yy Newtons of thrust', the FMs look more like 'propulsion line welds fail due to over-pressure' and the PACTs look more like 'perform weld inspections'.

The DDP methodology remains in synchronization with the evolving project design and one doesn't try to know what isn't yet known. This idea is incorporated into the tool development, in which the tool has a 'tree' structure of requirements, failure modes and PACTs. The tool provides pull-down menu choices which can be selected and formed into a more project-specific hierarchal relationship. The tool also allows for the input of new, or unique, attributes. This tends to come in more at lower levels of requirements (which tend to be project unique).

One big advantage of lower-level evaluations is the reduced reliance on engineering judgement (Delphi methods) and the ability to populate the matrices with real data or physics-based answers rather than the 1,3,9 non-linear qualitative scale necessary at higher levels. Note however, that many portions of one-of-a-kind spacecraft hardware design will always rely on engineering judgement and the DDP process seamlessly incorporates quantitative and qualitative data.

Example of DDP Application

The DDP process was recently applied, using the new software tool, to an advanced technology under development by NASA. The results of this application are illustrative of the DDP overall process, including utilization of the results. Figure 8 depicts .. 'screen shot' of the DDP tool after evaluation of this technology. A few comments about the different portions of the screen are in order:

PACTs

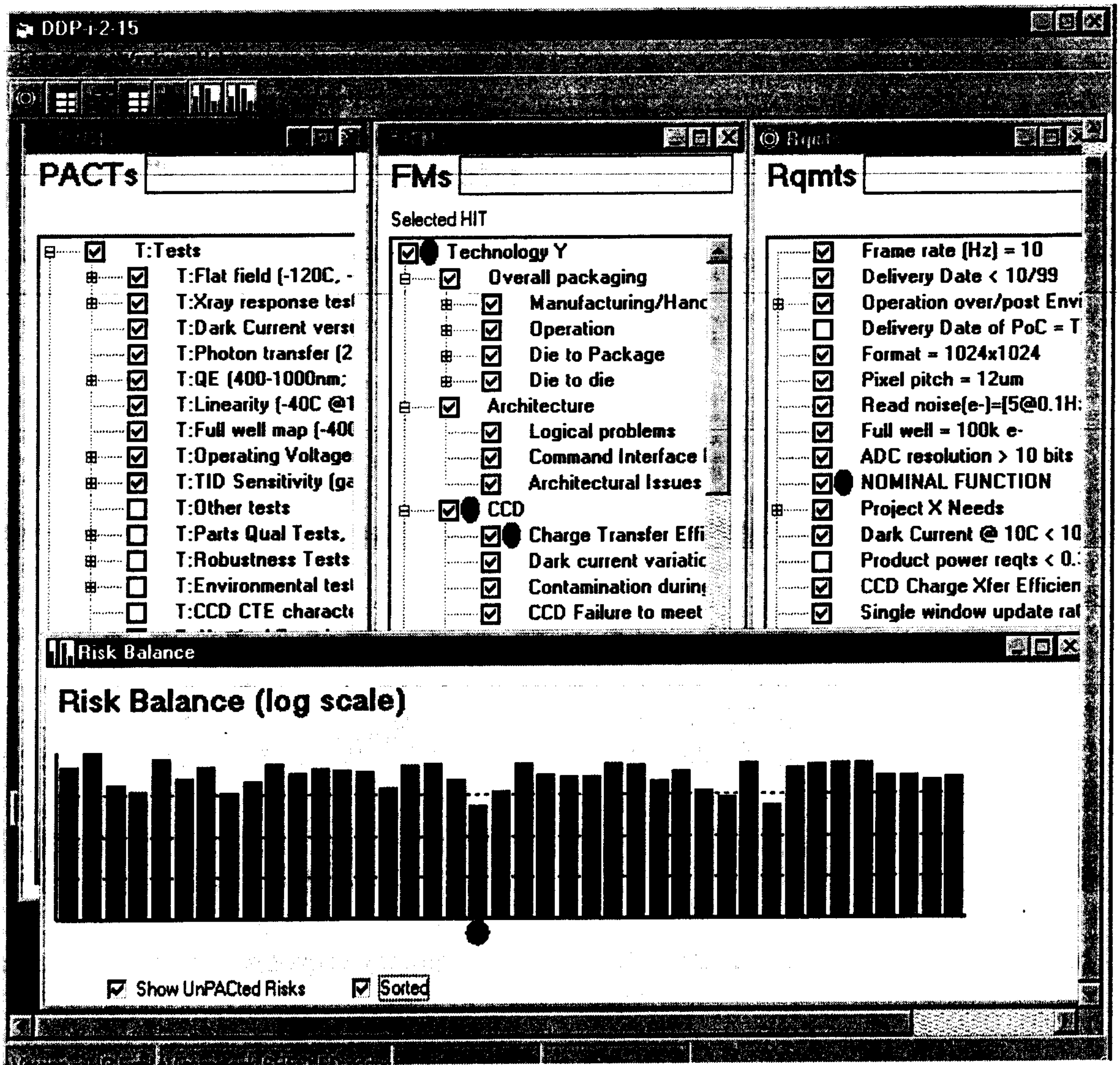
- In the PACTs list, only Tests are visible and a number of choices have been selected by the project (these have check marks).
- Some of the PACTs have sub-PACTs, that is aspects of the PACTs which could be added or subtracted to increase or decrease the effectiveness versus specific failure modes.

FMs

- The FMs are grouped logically (may depend on the specific application), e.g. Packaging includes a number of subordinate FMs including Manufacturing, Operation, Environmental interactions, etc.

Requirements

- Some of the requirements are not selected (no check marks) due to the customers recognizing that some of these requirements were driving the technology development before it even reached proof of concept stage. This is another utility of the requirements matrix, namely it can identify requirement drivers giving the project a chance to change or back-off some initial proposed requirements.



DDP-i-2-15

PACTs

☑ T:Tests
☑ T:Flat field (-120C, -
☑ T:Xray response test
☑ T:Dark Current versı
☑ T:Photon transfer (2
☑ T:QE (400-1000nm;
☑ T:Linearity (-40C @1
☑ T:Full well map (-40C
☑ T:Operating Voltage
☑ T:TID Sensitivity (ga
□ T:Other tests
□ T:Parts Qual Tests,
□ T:Robustness Tests
□ T:Environmental test
□ T:CCD CTE characte

FMs

Selected HIT

☑ ● Technology Y
☑ Overall packaging
☑ Manufacturing/Hanc
☑ Operation
☑ Die to Package
☑ Die to die
☑ Architecture
☑ Logical problems
☑ Command Interface I
☑ Architectural Issues
☑ ● CCD
☑ ● Charge Transfer Effi
☑ Dark current variatic
☑ Contamination durin
☑ CCD Failure to meet

Rqmts

☑ Frame rate (Hz) = 10
☑ Delivery Date < 10/99
☑ Operation over/post Envi
□ Delivery Date of PoC = T
☑ Format = 1024x1024
☑ Pixel pitch = 12um
☑ Read noise(e-)=(5@0.1H:
☑ Full well = 100k e-
☑ ADC resolution > 10 bits
☑ ● NOMINAL FUNCTION
☑ Project X Needs
☑ Dark Current @ 10C < 10
□ Product power reqts < 0.
☑ CCD Charge Xfer Efficien
☑ Single window update rat

Risk Balance

Risk Balance (log scale)

☑ Show UnPACted Risks ☑ Sorted

Figure 8. Sample output of the DDP tool (alpha version) after evaluation of a NASA advanced technology.

Risk Balance

- The residual risk is shown on the bottom of the screen display and illustrates what the risk would be with no PACTs applied (light shading) and with PACTs applied (dark shading). One can now focus on the remaining significant issues and stop worrying about the less significant ones.

Conclusions

NASA's Office of Safety and Mission Assurance is aggressively pursuing managing risk as a resource and has a Program in place to reach this goal. The idea of using Risk Balancing profiles for very early Mission Assurance tailoring is achieving acceptance and this process has been dove-tailed with the DDP process. The DDP process is being incorporated into a user-friendly tool. Pilot applications of this tool to date have demonstrated it's utility and ease of use (one application resulted in cost savings of 25x and a 3 year schedule improvement). The combination of RBPs and DDP process[2] promise to enable Risk Management from the mission level down to the lowest level of assembly and everything in between. RBPs allow early risk management planning in order to tailor the project's mission assurance program to ~~put~~ fit ~~this~~ the project constraints. DDP is an iterative tool which permits fine tuning of the risk management process. The DDP tool allows highly informed and specific risk decisions to be made based on actual identified failure modes and control of the risk they present.

then

Acknowledgements

The research described in this paper was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration through NASA's Office of Safety and Mission Assurance, Code Q. In particular, Dr. Michael Greenfield has been both advocate and sponsor of this effort from the beginning and has facilitated its development.

References

[1] M. Greenfield, Risk Balancing Profile Guide, this conference.
[2] See for example http://ise.larc.nasa.gov